Refine Search

Search Results -

Term	Documents
RTSP	144
RTSPS	11
MONITOR$	0
MONITOR	121370
MONITORABILITY	5
MONITORABLE	246
MONITORABLELINEDATA	1
MONITORABLELINEDATAINFO	1
MONITORABLE/CONTROLLABLE	3
MONITORABLY	3
MONITORAGE	3
(L9 AND (MONITOR$ WITH RTSP)).USPT.	0

There are more results than shown above. Click here to view the entire set.

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L11

Refine Search

Recall Text Clear Interrupt

Search History

DATE: Sunday, February 06, 2005 Printable Copy Create Case

Set Name side by side	**Query**	**Hit Count**	**Set Name** result set
	DB=USPT; PLUR=YES; OP=ADJ		
L11	L9 and (monitor$ with RTSP)	0	L11

L10	L9 and (monitor$ with transmit$ with protocol$)	50	L10
L9	L1 and (transmit$ with (error$ or fail$))	6769	L9
L8	L1 (transmit$ with (error$ or fail$))	0	L8
L7	L1 and (monitor$ with transmit$ with ptotocol)	0	L7
L6	L3 and (monitor$ with transmit$ with ptotocol)	0	L6
L5	L3 and (monitor$ with ptotocol)	0	L5
L4	L3 and (transmi$ with fail$)	0	L4
L3	L1 and (stream adj1 control adj1 protocol)	3	L3
L2	L1 and (stream adj1 control adj1 ptotocol)	0	L2
L1	709/$.ccls. or 714/$.ccls.	40216	L1

END OF SEARCH HISTORY

Previous Doc Next Doc Go to Doc#
First Hit Fwd Refs

Generate Collection

L10: Entry 7 of 50 File: USPT Feb 11, 2003

DOCUMENT-IDENTIFIER: US 6519223 B1
**** See image for Certificate of Correction ****
TITLE: System and method for implementing a semi reliable retransmission protocol

Brief Summary Text (5):
There are many applications where large volumes of digital data must be transmitted and received in a substantially error free manner. In telecommunications and satellite communications systems, in particular, it is imperative that the transmission of digital data over the air interface be completed in as accurate a manner as is possible. Accurate transmission and reception of digital data has, however, been difficult because the communications channels utilized for data transmissions over the air interface are plagued by error introducing factors. For example, such errors may be attributable to transient conditions in the channel, such as noise and distortion, or they may be due to recurrent conditions attributable to defects in the channel. The existence of transient conditions or defects results in instances where the digital data is not transmitted properly or cannot be reliably received.

Brief Summary Text (7):
Considerable attention has been directed toward discovering methods for addressing the problems concerning errors which typically accompany data transmission activities over the air interface. For example, two common techniques of error correction include Forward Error Correction (FEC) and Automatic Repeat Request (ARQ). The FEC error correction technique adds redundant information in the transmitter, which is used by the receiver to correct transmission errors, whereas in the (ARQ) error correction technique, the receiver requests retransmission of data packets not correctly received from the transmitter. Typically, a combination of FEC and ARQ techniques are applied to recover from transmission errors. The applied ratio of FEC verses ARQ depends upon the type of data being transmitted. For instance, real time data with strong requirements on small delay, such as voice, are normally carried with only FEC. On the other hand, for data with loose requirements with respect to delay, such as file transfers, usually a combination of FEC and ARQ is applied to maximize the probability of correct delivery.

Detailed Description Text (7):
When the physical layer 70a of the transmitter 200 transmits the PDUs 220 containing the data 215 over the air interface 240 to the receiver 250, the communications channel 245 between the transmitter 200 and receiver 250 used to transmit the data 215 may introduce a number of errors into the transmitted data 215. Several different types of error detection and correction techniques can be utilized by the transmitter 200 and receiver 250 to prevent data 215 loss.

Current US Cross Reference Classification (1):
714/749

CLAIMS:

1. A telecommunications system for transmitting data packets using a semi-reliable retransmission protocol that utilizes selective repeat automatic repeat request,

comprising: a transmitter having a data link layer therein for receiving a service data unit containing a plurality of said data packets, said data link layer segmenting said service data unit into at least one protocol data unit; a discard timer within said transmitter for monitoring a retransmission time of said at least one protocol data unit, said discard timer being initialized when said service data unit is received by said data link layer; and a receiver for receiving said at least one protocol data unit from said transmitter over an air interface and transmitting an acknowledgment message to said transmitter over said air interface after determining that said at least one protocol data unit is received correctly, said service data unit being discarded by said transmitter and said receiver when said acknowledgment message is not transmitted for said at least one protocol data unit and said discard timer expires.

26. A receiver for receiving data packets over an air interface from a transmitter using a semi-reliable retransmission protocol that utilizes a selective repeat automatic repeat request technique, comprising: means for receiving at least one protocol data unit segmented from a service data unit containing a plurality of said data packets from said transmitter over said air interface; means for transmitting an acknowledgment message to said transmitter over said air interface after determining that said at least one protocol data unit is received correctly; means for requesting retransmission of each said at least one protocol data unit that is received incorrectly using said selective repeat automatic repeat request technique; means for receiving a discard message from said transmitter when a discard timer monitoring the retransmission time of said at least one protocol data unit expires prior to the transmission of said acknowledgment message; and means for discarding said service data unit upon receipt of said discard message.

36. A method for receiving data packets over an air interface from a transmitter using a semi-reliable retransmission protocol that utilizes a selective repeat automatic repeat request technique, comprising the steps of receiving at least one protocol data unit segmented from a service data unit containing a plurality of said data packets from said transmitter over said air interface; transmitting an acknowledgment message to said transmitter over said air interface after determining that said at least one protocol data unit is received correctly; requesting retransmission of each said at least one protocol data unit that is received incorrectly using said selective repeat automatic repeat request technique; receiving a discard message from said transmitter when a discard timer monitoring the retransmission time of said at least one protocol data unit expires prior to the transmission of said acknowledgment message; and discarding said service data unit upon receipt of said discard message.

Previous Doc Next Doc Go to Doc#

US006519223B1

(12) United States Patent
Wager et al.

(10) Patent No.: US 6,519,223 B1
(45) Date of Patent: Feb. 11, 2003

(54) SYSTEM AND METHOD FOR IMPLEMENTING A SEMI RELIABLE RETRANSMISSION PROTOCOL

(75) Inventors: Stefan Henrik Andreas Wager, Helsinki (FI); Reiner Ludwig, Kensington, CA (US)

(73) Assignee: Telefonaktiebolaget L M Ericsson (publ), Stockholm (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/287,392

(22) Filed: Apr. 6, 1999

(51) Int. Cl.[7] H04L 1/18

(52) U.S. Cl. 370/216; 714/749

(58) Field of Search 370/469, 389, 370/395, 278, 216; 714/748, 749, 750

(56) References Cited

U.S. PATENT DOCUMENTS

5,222,061 A 6/1993 Doshi et al. 370/13
5,684,791 A * 11/1997 Raychaudhuri et al. 370/278
5,754,754 A 5/1998 Dudley et al. 395/182.16
6,198,746 B1 * 3/2001 Saito 370/398
6,256,300 B1 * 7/2001 Ahmed et al. 370/331
6,424,625 B1 * 7/2002 Larsson et al. 370/236

FOREIGN PATENT DOCUMENTS

EP 1 006 689 A2 6/2000

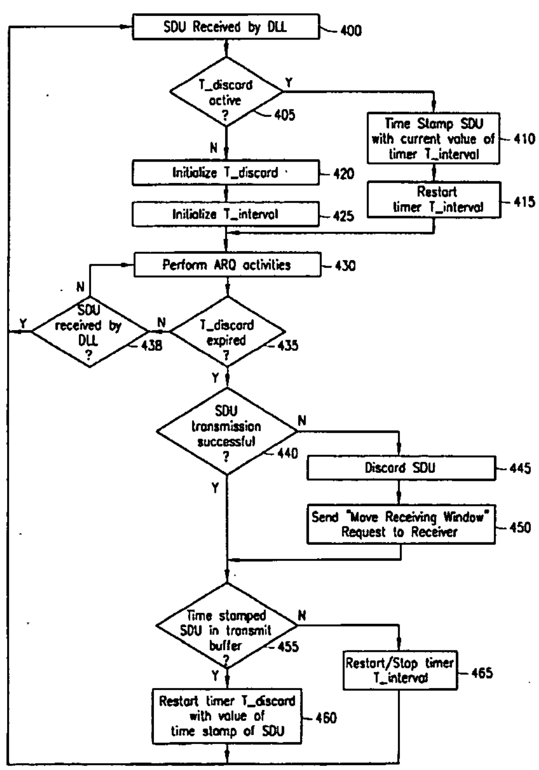
* cited by examiner

Primary Examiner—Ken Vanderpuye
(74) Attorney, Agent, or Firm—Jenkens & Gilchrist, P.C.

(57) ABSTRACT

A telecommunications system and method is disclosed for implementing a semi-reliable retransmission protocol that utilizes both selective repeat Automatic Repeat Request (ARQ) and segmentation and assembly of data packets. The new semi-reliable retransmission protocol includes a timer based triggering of a retransmission timeout for retransmission protocols, which allows the retransmission timeout to become insensitive to variations in the channel rate. In addition, the retransmission timeout can be defined based upon the maximum delay allowable for the retransmission of corrupted data packets over the air interface. For every data packet received a timer monitoring the transmission time of the data packet is initialized. If the timer elapses for the data packet this data packet is marked as discarded in the transmitter, and a request is sent to the receiver to ensure that transmissions carrying that data packet are discarded in the receiver.

37 Claims, 5 Drawing Sheets



L10: Entry 8 of 50 File: USPT Dec 3, 2002

DOCUMENT-IDENTIFIER: US 6490641 B2
TITLE: Addressable shadow port circuit

Detailed Description Text (81):
After enabling the transmitter circuit to send the select protocol, the master control circuit transitions from the Transmit Select Protocol state to the Receive Acknowledge Protocol state. In the Receive Acknowledge Protocol state, the master control circuit enables the SBM's receiver circuit to receive the acknowledge protocol from the selected ASP. After the acknowledge protocol is received, the master control circuit transitions from the Receive Acknowledge Protocol state into the Expected Address Received? state to verify that the address of the selected ASP was received. If an incorrect address was received, the master control circuit aborts the board select operation and transitions from the Expected Address Received? state into the Report Address Error state. In the Report Address Error state, the master control circuit reports the address failure and places the SBM's transmitter and receiver circuits into their idle state.

Detailed Description Text (134):
The Type 1 select protocol message frame consists of a header comprising a RCASP address and command field, and a cyclic redundancy check (CRC) value field. The CRC field is optional and may be removed if error detection is not required. The RCASP address and command fields in the header are separated by an S signal, and the CRC field is separated from the header by a S signal. The Type 2 message frame shown in FIG. 24 includes one or more optional fields between the header and the CRC field as required by the command sent in the header. The optional fields are also separated by an S signal. The header and optional fields can be transmitted in either fixed or variable D signal bit-pair length, although for error detection a fixed field length is preferred, since it is easier to calculate CRCs on fixed length data fields than on variable length data fields.

Detailed Description Text (138):
FIG. 25 depicts the example messages using the expanded acknowledge protocol of the invention. The Type 1 acknowledge protocol message frame consists of a header comprising a RCASP address and status field and a CRC field. The address field identifies the RCASP which is transmitting the acknowledge message, and the status field informs the PSBM of the status of the RCASP. The CRC field is optional and may be removed if error detection is not required. The address and status fields in the header are separated by an S signal, and the CRC field is separated from the header by a S signal. The Type 2 message frame includes one or more optional fields between the header and the CRC field as required by the command sent in the previous select protocol. The optional fields are also separated by an S signal. The header and optional fields can be transmitted in either fixed or variable D signal bit-pair length, although for error detection a fixed field length is preferred, since it is easier to calculate CRCs on fixed length data fields than on variable length data fields.

Detailed Description Text (147):
After the select protocol has been transmitted, the RCASP outputs a Connect PSBM command acknowledge protocol to the PSBM with a message frame containing a header

consisting of the RCASP's address (ADD) and status register (STS), and a CRC field as seen in FIG. 26. The CRC field transmitted in the acknowledge protocol is calculated by the RCASP doing a check sum on the address and status fields transmitted in the acknowledge protocol. After the acknowledge protocol is transmitted and if a CRC error has not occurred in the select protocol, the Connect PSBM command causes the RCASP to connect the primary and secondary ports. After the connection is made, the PSBM can access the board's serial bus using the 1149.1 serial bus protocol. If a CRC error occurred in the select protocol, the RCASP outputs the acknowledge protocol, bus does not make a connection between the primary and secondary ports.

Detailed Description Text (154):
After the select protocol has been transmitted, the RCASP outputs a Disconnect PSBM command acknowledge protocol to the PSBM with a message frame containing a header consisting of the RCASP's address (ADD) and status register (STS), and a CRC field as seen in FIG. 26. The CRC field transmitted in the acknowledge protocol is calculated by the RCASP by doing a check sum on the address and status fields transmitted in the acknowledge protocol. After the acknowledge protocol is transmitted and if a CRC error has not occurred in the select protocol, the Disconnect PSBM command causes the RCASP to disconnect the primary and secondary ports. If a CRC error occurred in the select protocol, the RCASP outputs the acknowledge protocol, bus does not disconnect the primary and secondary ports.

Detailed Description Text (161):
After the acknowledge protocol is transmitted and if no CRC error occurred in the select protocol, the Connect RSBM command causes the RCASP to set the RENA output to the RSBM and connect the remote and secondary ports. In response to the RENA signal being set, the RSBM is enabled to access the board's serial bus using the 1149.1 serial bus protocol. While the RSBM is busy accessing the serial bus, the PSBM is free to do other tasks.

Detailed Description Text (168):
After the acknowledge protocol is transmitted and if no CRC error occurred in the select protocol, the Disconnect RSBM command causes the RCASP to reset the RENA output to the RSBM and disconnect the remote and secondary ports. In response to the RENA signal being reset, the RSBM is disabled from accessing the board's serial bus using the 1149.1 serial bus protocol.

Detailed Description Text (174):
In response to the RCASP acknowledge protocol, the PSBM checks for CRC errors, address errors, and status errors as described in the Connect PSBM command description. If no errors are found the PSBM is assured that the RCASP has correctly received the Read Status command, executed the command, and transmitted the contents of the status register. In response to an error, the PSBM can re-send the Read Status command to the RCASP.

Detailed Description Text (317):
After the enabling the transmitter circuit to send the hierarchical select protocol, the master control circuit transitions from the Transmit Hierarchical Select Protocol state to the Receive Hierarchical Acknowledge Protocol state. In the Receive Hierarchical Acknowledge Protocol state, the master control circuit enables the SBM's receiver circuit to receive the hierarchical acknowledge protocol from the selected HASP/ASP devices. After the hierarchical acknowledge protocol is received, the master control circuit transitions from the Receive Hierarchical Acknowledge Protocol state into the Expected Addresses Received? state to verify that the address frames were correctly received. If incorrect addresses were received, the master control circuit aborts the select operation and transitions from the Expected Addresses Received? state into the Report Address/Time Out Error state. In the Report Address/Time Out Error state, the master control circuit reports the address failure and places the SBM's transmitter and receiver circuits

into their idle state.

Detailed Description Text (320):
Note that if the hierarchical acknowledge protocol is not received after a predetermined amount of time, the master control circuit can transition from the Receiver Hierarchical Acknowledge Protocol state to the Transmit Hierarchical Select Protocol state in response to the Time Out Error and transmit a hierarchical select protocol with reset address frames into the HASPs of the system, as described above. After transmitting the reset address frames, the master control circuit transitions from the Transmit Hierarchical Select Protocol state to the Report Address/Time Out Error state to report the time out failure, place the SBM's transmitter and receiver circuits in their idle states, and then transition into the Master Control Circuit Idle state.

Detailed Description Text (328):
A state diagram of the operation of the HASP's transmitter circuit is shown in FIG. 43. The HASP uses its transmitter circuit to transmit the hierarchical acknowledge protocol and to transfer serial data during 1149.1 serial bus operations. In the state diagram, the transmitter circuit is forced into the Transmitter Disabled state while the 1149.1 bus is active. This state insures that the transmitter cannot be inadvertently enabled, while the 1149.1 bus is in operation, to output the hierarchical select protocols. When the 1149.1 bus is idle, the transmitter circuit enters into the Transmitter Idle state. In the Transmitter Idle state, three scenarios can occur. (1) If it is not necessary to output an acknowledge protocol, the transmitter circuit remains in the Transmitter Idle state until the 1149.1 bus becomes active again, in which case the transmitter circuit returns to the Transmitter Disabled state. (2) If the previous select protocol was not hierarchical (HSP Flag is reset see section 4.2), the transmitter circuit enters the Send 1st I Signal state (a) to output the first I signal to start the acknowledge protocol, then enters the Send 1st S Signal state (a) to output the first S signal to start the address frame, then enters the Send Address Frame state (a) to output a series of D signals indicating the HASP address, then enters the Send 2nd S Signal state (a) to output the second S signal to stop the address frame. The transmitter circuit transitions from the Send 2nd S Signal state (a) to the Send 2nd I Signal state to stop the acknowledge protocol. From the Send 2nd I Signal state, the transmitter circuit returns to the Transmitter Idle state. The transmitter returns to the Transmitter Disabled state whenever the 1149.1 bus becomes active again. (3) If the previous select protocol was hierarchical (HSP Flag is set, see section 4.2), the transmitter circuit enters the Poll For 1st S Signal state to monitor the STDI input for the start of an acknowledge protocol. The transmitter circuit remains in the Poll For 1st S Signal state while I signals are input on the STDI input. If the 1149.1 bus becomes active or if a time out error occurs, the transmitter will transition into the Transmitter Idle state. If an S Signal is received on the STDI input, the transmitter circuit enters the Send 1st I Signal state (b) to output the first I signal on PTDO to start the acknowledge protocol, then enters the Send 1st S Signal state (b) to output the first S signal to start relaying the received address frame from an ASP or message frame from a RCASP, then enters the Relay Address Frame state to relay a series of D signals received on the STDI input to the PTDO output. When a 2nd S signal is received on the STDI input, the transmitter circuit enters the Send 2nd S Signal state (b) to output the second S signal on the PTDO output to stop relaying the address or message frame. One of the following scenarios occur after the 2nd S signal has been received. (1) If the next signal received on the STDI input is a D signal, message frame fields are being received and the transmitter re-enters the Relay Address Frame state (b) and continues the process of relaying message frame fields. (2) If the next signal received on the STDI input is an S signal, the first frame type (address or message type) has been relayed and another address frame is being received. To relay the next address frame, the transmitter re-enters the Send 1st S Signal state to start relaying the next address frame. The transmitter pauses in the Send 1st S Signal state if additional S signals are input. (3) If the next

signal received on the STDI input is a 2nd I signal, the transmitter enters the Send 1st S Signal state (a) to output a 1st S Signal to start its own address frame, then enters the Send Address Frame to output its address frame, then enters the Send 2nd S Signal state (a) to output the second S signal to stop its address frame output. The transmitter transitions from the Send 2nd S Signal state (a) to the Send 2nd I Signal state to stop the hierarchical acknowledge protocol. From the Send 2nd I Signal state, the transmitter circuit returns to the Transmitter Idle state. The transmitter returns to the Transmitter Disabled state whenever the 1149.1 bus becomes active again.

Detailed Description Text (335):
Note that if the hierarchical acknowledge protocol is not received after a predetermined amount of time, the HASP's transmitter circuit will terminate the acknowledge protocol and input a time out error signal to the slave control circuit, as described above. In response to the time out error signal, the slave control circuit will transition from the Relay Hierarchical Acknowledge Protocol state into the Slave Control Circuit Idle state and wait for another hierarchical select protocol input from the SBM.

Detailed Description Text (351):
After the last frame of a hierarchical acknowledge protocol has been relayed from the STDI input to the PTDO output, via flipflops 5 and 6, MX1 selects the APO output from the transmitter to send the HASP's address frame and then terminates the hierarchical acknowledge protocol. During 1149.1 scan operations, MX1 selects the STDI input that passes through FF7. FF7 is clocked by PTCK and provides the synchronization required for hierarchical scan access, as described above with respect to FIG. 38. When disabled by control input from the slave control circuit, the PTDO output from the buffer 3SB is pulled up to a logic 1 level by a pull-up resistor inside the buffer. The status output from the transmitter circuit indicates to the slave control circuit when a hierarchical acknowledge protocol has been started, when the last hierarchical address frame has been relayed, and if a time out error has occurred during a hierarchical acknowledge protocol. The control input to the transmitter from the slave control circuit enables the transmitter for acknowledge operations and inputs the HSP flag to indicate whether the acknowledge protocol is a hierarchical or non-hierarchical type.

Current US Cross Reference Classification (1):
714/30

Previous Doc Next Doc Go to Doc#

US006490641B2

(12) **United States Patent**
Whetsel

(10) **Patent No.: US 6,490,641 B2**
(45) **Date of Patent: Dec. 3, 2002**

(54) **ADDRESSABLE SHADOW PORT CIRCUIT**

(75) Inventor: **Lee D. Whetsel**, Plano, TX (US)

(73) Assignee: **Texas Instruments Incorporated**, Dallas, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/997,327**

(22) Filed: **Nov. 29, 2001**

(65) **Prior Publication Data**

US 2002/0035658 A1 Mar. 21, 2002

Related U.S. Application Data

(62) Division of application No. 09/253,505, filed on Feb. 19, 1999, now Pat. No. 6,363,443, which is a division of application No. 08/485,741, filed on Jun. 7, 1995, now Pat. No. 5,875,353, which is a continuation of application No. 08/427,947, filed on Apr. 24, 1995, now Pat. No. 5,483,518, which is a continuation of application No. 08/322,112, filed on Oct. 12, 1994, now abandoned, which is a continuation of application No. 07/900,708, filed on Jun. 17, 1992, now abandoned.

(51) **Int. Cl.**^{7} **G06F 13/00**; G06F 11/00
(52) **U.S. Cl.** **710/104**; 714/30
(58) **Field of Search** 710/8, 9, 10, 104, 710/107; 714/30, 36, 724; 370/241, 251

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,873,818	A	3/1975	Barnard
3,976,940	A	8/1976	Chau et al.
4,023,142	A	5/1977	Woessner
4,066,882	A	1/1978	Esposito
4,146,835	A	3/1979	Chnapko et al.
4,264,807	A	4/1981	Moen et al.
RE31,056	E	10/1982	Chau et al.
4,357,703	A	11/1982	Van Brunt
4,390,969	A	6/1983	Hayes

(List continued on next page.)

OTHER PUBLICATIONS

Bhavasar, D., "An Architecture for Extending the IEEE Standard 1149.1 Test Access Port to System Backplanes", International Test Conference 1991, pp. 768–776.

Bhavsar, et al., "Self-Testing by Polynomial Division", Digest of Papers, International Test Conference, 1981, pp. 208–216.

El-ziq, et al., "A Mixed-Mode Built-In Self-Test Technique Using Scan Path and Signature Analysis", International Test Conference, Oct. 18–20, 1983, pp. 269–274.

Haedtke, et al., "Multilevel Self-test for the Factory and Field", Proceedings, Annual Relability and Maintainability Symposium, 1987.

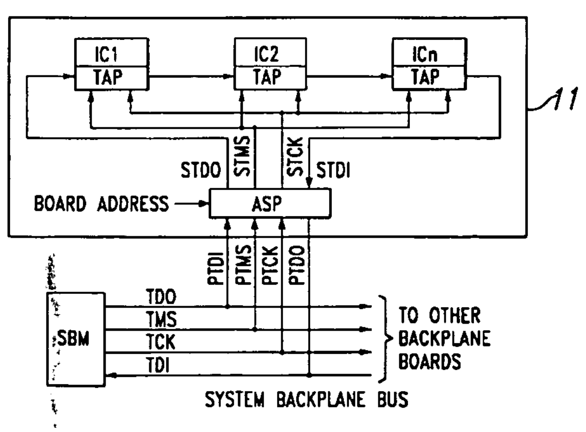
(List continued on next page.)

Primary Examiner—Glenn A. Auve
(74) *Attorney, Agent, or Firm*—Lawrence J. Bassuk; W. James Brady; Frederick J. Telecky, Jr.

(57) **ABSTRACT**

A protocol and associated circuitry operable for efficiently extending serial bus capability in system environments is disclosed. The protocol is designed to coexist and be fully compatible with existing serial bus approaches, and in particular an example of application of the invention to a backplane system utilizing the 1149.1 IEEE standard serial bus is detailed. The circuitry and protocol required to couple any one of the boards on the backplane to the serial bus master without modifying the existing serial bus protocol, without adding additional signals, and without affecting the throughput rate of the serial bus is described. The invention advantageously allows the serial bus master to select, communicate with, and deselect backplane boards so that high level test functions may be simultaneously executed and monitored. Additional preferred embodiments are also disclosed.

2 Claims, 21 Drawing Sheets



Previous Doc Next Doc Go to Doc#
First Hit Fwd Refs

Generate Collection

L10: Entry 9 of 50 File: USPT Aug 6, 2002

DOCUMENT-IDENTIFIER: US 6430711 B1
TITLE: System and method for monitoring the state of a plurality of machines connected via a computer network

Detailed Description Text (5):
In the machine monitor system 1 according to the embodiment in the connection described, the agent unit 10 and the console unit 20 support SMTP and POP3 of standard protocols for transmitting and receiving electronic mail through the Internet 6 and MAP1 provided as an interface for transmitting and receiving electronic mail through the Internet 6 enables electronic mail to be exchanged between the units. Specifically, the agent unit 10 gets status information .O slashed.1 indicating the operation state of each network printer P connected to the LAN 3a and the toner remaining amount, the ink remaining amount, photosensitive drum remaining life, etc., and prepares status mail (electronic mail) .O slashed.2 storing the status information .O slashed.1. It adds the address of the console unit 20 to the status mail .O slashed.2 and sends the status mail .O slashed.2 via the router 4 to the Internet 6. Then, the status mail .O slashed.2 is stored in the mail server 19 of the provider with which the agency contracts. Status mail .O slashed.2 addressed to the console unit 20 from other agent units 10 is also stored in the mail server 19. The console unit 20 reads at a proper timing a large number of pieces of the status mail .O slashed.2 stored in the mail server 19.

Detailed Description Text (20):
The control section 15 operates the local information getting section 11, the local information retention section 12, the local information transmission section 13, the display section 14, the input section 16, and the timer monitor section 17 for causing the sections to perform the required operation. The control section 15 registers customer information entered through the input section 16 in the customer information retention section 18, creates a printer registration log file 12c based on printer relevant information entered through the input section 16, stores the file in the local information retention section 12, creates a status log file 12a based on the status information .O slashed.1 gotten by the local information getting section 11, stores the file in the local information retention section 12, records a communication history in the local information transmission section 13 in the transmission log file 12b, and stores the transmission log file 12b in the local information retention section 12. The control section 15 looks up in the error table in the error table retention section 9 (FIG. 20) to determine the error level corresponding to the status information .O slashed.1 in the status log file 12a. If the control section 15 determines that the error level is fatal, it creates a fatal error log file 12d and stores the file in the local information retention section 12. Further, the control section 15 causes the local information getting section 11 to get the status information .O slashed.1 every first time period T1 and causes the local information transmission section 13 to transmit status mail every second time period T2 longer than the first time period T1. If the control section 15, as the status determination means, determines that the error level corresponding to the status information .O slashed.1 gotten from one network printer P is fatal (status code>6000), it instructs the local information transmission section 13 to transmit status mail storing the contents of the fatal error log file 12d (fatal error occurrence mail). The control section 15 also

instructs the local information getting section 11 to get the status information .O slashed.1 every minute from the network printer P with status code>6000 (the error level corresponding to the status information .O slashed.1 is fatal). Further, if the error level corresponding to the status information .O slashed.1 gotten from one network printer P is not fatal any longer, the control section 15 instructs the local information transmission section 13 to transmit status mail indicating the fact (fatal error recovery mail). Further, if the control section 15, as the status determination means, determines that the state in which the error level corresponding to the status information .O slashed.1 gotten from one network printer P is fatal exceeds one hour, it judges that the user cannot correct the error and that it is necessary to request the agency to dispatch maintenance personnel, and immediately causes the local information transmission section 13 to transmit status mail indicating the request for dispatching maintenance personnel (service call error mail).

Detailed Description Text (71):
At step S126, the CPU 30 stores the information described in the fatal error log file 12d in status mail (fatal error occurrence mail) .O slashed.2 shown in FIG. 22 and transmits the status mail .O slashed.2 to the mail server 19 (address of the console unit 20) (as a local information transmission step). As shown in FIG. 22, the status mail .O slashed.2 consists of a mail header of subject indicating status mail and mail address and one or more mail texts prepared for each network printer P. Each mail text consists of the serial number of the corresponding network printer P, the contents of the status information .O slashed.1 (namely, status code, remaining amount information of toner remaining amount, ink remaining amounts, etc., and the like), and the information getting date and time indicating the point in time at which the status information .O slashed.1 was gotten. If the status mail .O slashed.2 is prepared based on the fatal error log file 12d, the status information .O slashed.1 other than the status code is not contained in the fatal error log file 12d, thus the fields of the status information .O slashed.1 other than the status code in each mail text remain blank.

Detailed Description Text (76):
In contrast, if the CPU 30 determines at step S128 that the fatal error log file 12d contains the record of the target printer, namely, if the fatal error that once occurred is corrected, the CPU 30 goes to step S129 and deletes the record of the target printer from the fatal error log file 12d. At step S130, the CPU 30 executes the status mail transmission subroutine in FIG. 9, thereby storing the information described in the fatal error log file 12d in the status mail (fatal error recovery mail) .O slashed.2 and transmitting the status mail .O slashed.2 to the mail server 19 (address of the console unit 20) (as a local information transmission step). After completion of step S130, the CPU 30 advances the process to step S133.

Detailed Description Text (83):
At step S114, the CPU 30 changes the status code (>6000) described on the record with the elapsed time exceeding one hour to "XXXX" representing a service call error. At step S115, the CPU 30 executes the status mail transmission subroutine in FIG. 9, thereby storing the information described in the fatal error log file 12d in the status mail .O slashed.2 and transmitting the status mail (service call error mail) .O slashed.2 to the mail server 19 (address of the console unit 20) (as a local information transmission step). The service call error mail requests the agency to dispatch maintenance personnel and there is little possibility that the user may be able to correct the error under circumstances where the service call error mail is transmitted. Then, at step S116, the CPU 30 deletes the record with the status code changed at step S114 from the fatal error log file 12d, then returns the process to step S101.

Detailed Description Text (152):
As shown in FIG. 24 and FIG. 25, at the normal time during which an error does not occur in the network printers 2, the agent unit 10 monitors each network printer P

at step S103 in a first time period T1 (for example, 10 minutes) shorter than a second time period T2 (for example, two hours) actually transmitting the status mail .O slashed.2 and always updates the status information .O slashed.1 from each network printer P recorded in the status log file 12a at step S120, then sends only the most recent status information .O slashed.1 at time of transmitting the status mail .O slashed.2 to the console unit 20 via the mail server 19 at step S110. Therefore, even if the status code in the status information .O slashed.1 becomes temporarily the status code indicating WARNING or INFORMATION before the status mail .O slashed.2 is transmitted, the status code is not sent to the console unit 20 if the status is canceled when the status mail .O slashed.2 is transmitted. Then, the operator of the console unit 20 (agency) is relieved of the inconvenience of a temporary error.

Detailed Description Text (154):
If such a fatal error occurs, the agent unit 10 continues to monitor only the network printer P where the fatal error occurs in a time period (one minute) shorter than the normal monitor period (first time period T1) at steps S105 and S107, whereby the agent unit 10 can keep track of the status information .O slashed.1 more accurate than that in the normal state. If the fatal error is recovered from before the elapsed time since the fatal error occurrence exceeds one hour, immediately the agent unit 10 transmits status mail indicating the fact (fatal error recovery mail) to the console unit 20 via the mail server 19 at step S130. Therefore, the operator of the console unit 20 (agency) can cancel the emergency system adopted in response to the fatal error occurrence. In contrast, if the elapsed time since the fatal error occurrence exceeds one hour, immediately the agent unit 10 transmits status mail making a request for dispatching maintenance personnel (service call error mail) to the console unit 20 via the mail server 19 at steps S113 and S115. Therefore, the operator of the console unit 20 (agency) can dispatch maintenance personnel.

Current US Original Classification (1):
714/47

Previous Doc Next Doc Go to Doc#

US006430711B1

(12) **United States Patent**
Sekizawa

(10) **Patent No.: US 6,430,711 B1**
(45) **Date of Patent: Aug. 6, 2002**

(54) **SYSTEM AND METHOD FOR MONITORING THE STATE OF A PLURALITY OF MACHINES CONNECTED VIA A COMPUTER NETWORK**

(75) Inventor: **Hiroaki Sekizawa**, Suwa (JP)

(73) Assignee: **Seiko Epson Corporation**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/226,332**

(22) Filed: **Jan. 6, 1999**

(30) **Foreign Application Priority Data**

Jan. 6, 1998	(JP)	10-000694
Mar. 27, 1998	(JP)	10-081169
Mar. 27, 1998	(JP)	10-081170
Apr. 6, 1998	(JP)	10-093737
Apr. 6, 1998	(JP)	10-093738
Dec. 7, 1998	(JP)	10-347359

(51) **Int. Cl.**[7] **G06F 11/32**; G06K 15/00
(52) **U.S. Cl.** **714/47**; 358/1.14; 358/1.15
(58) **Field of Search** 714/47, 39; 709/217, 709/224, 223, 249, 238; 710/1, 105, 15, 62; 340/825.06, 286.02; 399/18; 700/169, 175, 108, 110; 370/908; 347/17, 101; 358/1.14, 1.15

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,251,858	A	*	2/1981	Cambigue et al.
5,077,582	A		12/1991	Kravette et al.
5,084,875	A		1/1992	Weinberger et al.
5,214,772	A		5/1993	Weinberger et al.
5,220,674	A	*	6/1993	Morgan et al.
5,305,199	A		4/1994	LoBiondo et al.
5,333,286	A		7/1994	Weinberger et al.
5,580,177	A	*	12/1996	Gase et al.
5,604,578	A		2/1997	Shibuya et al.
5,651,006	A		7/1997	Fujino et al.
5,727,135	A	*	3/1998	Webb et al.
5,859,778	A		1/1999	Kuroda et al.
5,982,994	A	*	11/1999	Mori et al.
6,088,816	A	*	7/2000	Nouri et al.

FOREIGN PATENT DOCUMENTS

JP	03-161765	7/1991
JP	04-256971	9/1992
JP	5-191405	7/1993
JP	05-236555	9/1993
JP	06-284150	10/1994
JP	06-348632	12/1994
JP	07-044630	2/1995
JP	07-288871	10/1995
JP	08-115125	5/1996
JP	08-241019	9/1996
JP	08-286854	11/1996
JP	09-134297	5/1997
JP	09-152815	6/1997
JP	9-188042	7/1997
JP	09-251356	9/1997

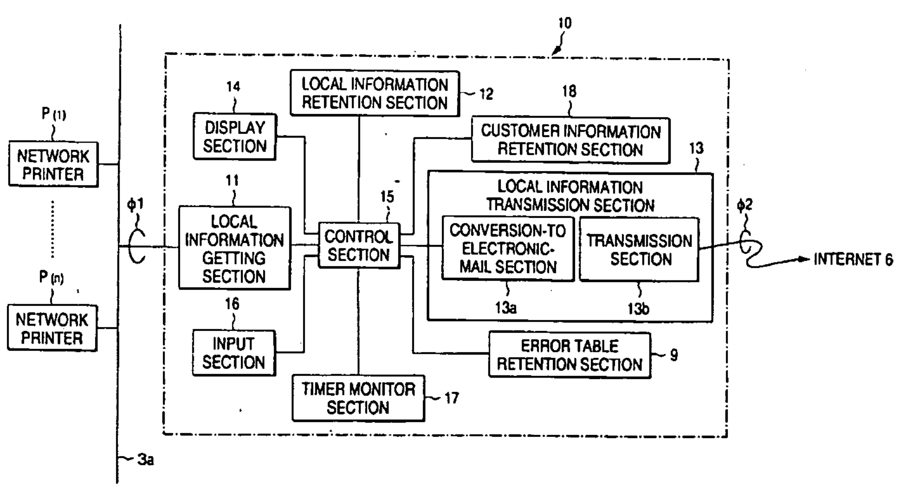
* cited by examiner

Primary Examiner—Gopal C. Ray
(74) *Attorney, Agent, or Firm*—Stroock & Stroock & Lavan LLP

(57) **ABSTRACT**

Each agent unit gets status information indicating the state of each of network printers connected by a LAN from the network printers every first time period. Whenever each agent unit gets the status information from the network printer, it overwrites a status log data file with the gotten status information. Each agent unit converts all status information stored in the status log data file into status mail of electronic mail and transmits the status mail to a mail server every second time period longer than the first time period. On the other hand, a console unit accesses the mail server and reads the status mail in a proper time period to the console unit.

69 Claims, 42 Drawing Sheets



L10: Entry 9 of 50 File: USPT Aug 6, 2002

DOCUMENT-IDENTIFIER: US 6430711 B1
TITLE: System and method for monitoring the state of a plurality of machines connected via a computer network

Detailed Description Text (5):
In the machine monitor system 1 according to the embodiment in the connection described, the agent unit 10 and the console unit 20 support SMTP and POP3 of standard protocols for transmitting and receiving electronic mail through the Internet 6 and MAP1 provided as an interface for transmitting and receiving electronic mail through the Internet 6 enables electronic mail to be exchanged between the units. Specifically, the agent unit 10 gets status information .O slashed.1 indicating the operation state of each network printer P connected to the LAN 3a and the toner remaining amount, the ink remaining amount, photosensitive drum remaining life, etc., and prepares status mail (electronic mail) .O slashed.2 storing the status information .O slashed.1. It adds the address of the console unit 20 to the status mail .O slashed.2 and sends the status mail .O slashed.2 via the router 4 to the Internet 6. Then, the status mail .O slashed.2 is stored in the mail server 19 of the provider with which the agency contracts. Status mail .O slashed.2 addressed to the console unit 20 from other agent units 10 is also stored in the mail server 19. The console unit 20 reads at a proper timing a large number of pieces of the status mail .O slashed.2 stored in the mail server 19.

Detailed Description Text (20):
The control section 15 operates the local information getting section 11, the local information retention section 12, the local information transmission section 13, the display section 14, the input section 16, and the timer monitor section 17 for causing the sections to perform the required operation. The control section 15 registers customer information entered through the input section 16 in the customer information retention section 18, creates a printer registration log file 12c based on printer relevant information entered through the input section 16, stores the file in the local information retention section 12, creates a status log file 12a based on the status information .O slashed.1 gotten by the local information getting section 11, stores the file in the local information retention section 12, records a communication history in the local information transmission section 13 in the transmission log file 12b, and stores the transmission log file 12b in the local information retention section 12. The control section 15 looks up in the error table in the error table retention section 9 (FIG. 20) to determine the error level corresponding to the status information .O slashed.1 in the status log file 12a. If the control section 15 determines that the error level is fatal, it creates a fatal error log file 12d and stores the file in the local information retention section 12. Further, the control section 15 causes the local information getting section 11 to get the status information .O slashed.1 every first time period T1 and causes the local information transmission section 13 to transmit status mail every second time period T2 longer than the first time period T1. If the control section 15, as the status determination means, determines that the error level corresponding to the status information .O slashed.1 gotten from one network printer P is fatal (status code>6000), it instructs the local information transmission section 13 to transmit status mail storing the contents of the fatal error log file 12d (fatal error occurrence mail). The control section 15 also

instructs the local information getting section 11 to get the status information .O slashed.1 every minute from the network printer P with status code>6000 (the error level corresponding to the status information .O slashed.1 is fatal). Further, if the error level corresponding to the status information .O slashed.1 gotten from one network printer P is not fatal any longer, the control section 15 instructs the local information transmission section 13 to transmit status mail indicating the fact (fatal error recovery mail). Further, if the control section 15, as the status determination means, determines that the state in which the error level corresponding to the status information .O slashed.1 gotten from one network printer P is fatal exceeds one hour, it judges that the user cannot correct the error and that it is necessary to request the agency to dispatch maintenance personnel, and immediately causes the local information transmission section 13 to transmit status mail indicating the request for dispatching maintenance personnel (service call error mail).

Detailed Description Text (71):
At step S126, the CPU 30 stores the information described in the fatal error log file 12d in status mail (fatal error occurrence mail) .O slashed.2 shown in FIG. 22 and transmits the status mail .O slashed.2 to the mail server 19 (address of the console unit 20) (as a local information transmission step). As shown in FIG. 22, the status mail .O slashed.2 consists of a mail header of subject indicating status mail and mail address and one or more mail texts prepared for each network printer P. Each mail text consists of the serial number of the corresponding network printer P, the contents of the status information .O slashed.1 (namely, status code, remaining amount information of toner remaining amount, ink remaining amounts, etc., and the like), and the information getting date and time indicating the point in time at which the status information .O slashed.1 was gotten. If the status mail .O slashed.2 is prepared based on the fatal error log file 12d, the status information .O slashed.1 other than the status code is not contained in the fatal error log file 12d, thus the fields of the status information .O slashed.1 other than the status code in each mail text remain blank.

Detailed Description Text (76):
In contrast, if the CPU 30 determines at step S128 that the fatal error log file 12d contains the record of the target printer, namely, if the fatal error that once occurred is corrected, the CPU 30 goes to step S129 and deletes the record of the target printer from the fatal error log file 12d. At step S130, the CPU 30 executes the status mail transmission subroutine in FIG. 9, thereby storing the information described in the fatal error log file 12d in the status mail (fatal error recovery mail) .O slashed.2 and transmitting the status mail .O slashed.2 to the mail server 19 (address of the console unit 20) (as a local information transmission step). After completion of step S130, the CPU 30 advances the process to step S133.

Detailed Description Text (83):
At step S114, the CPU 30 changes the status code (>6000) described on the record with the elapsed time exceeding one hour to "XXXX" representing a service call error. At step S115, the CPU 30 executes the status mail transmission subroutine in FIG. 9, thereby storing the information described in the fatal error log file 12d in the status mail .O slashed.2 and transmitting the status mail (service call error mail) .O slashed.2 to the mail server 19 (address of the console unit 20) (as a local information transmission step). The service call error mail requests the agency to dispatch maintenance personnel and there is little possibility that the user may be able to correct the error under circumstances where the service call error mail is transmitted. Then, at step S116, the CPU 30 deletes the record with the status code changed at step S114 from the fatal error log file 12d, then returns the process to step S101.

Detailed Description Text (152):
As shown in FIG. 24 and FIG. 25, at the normal time during which an error does not occur in the network printers 2, the agent unit 10 monitors each network printer P

at step S103 in a first time period T1 (for example, 10 minutes) shorter than a second time period T2 (for example, two hours) actually transmitting the status mail .O slashed.2 and always updates the status information .O slashed.1 from each network printer P recorded in the status log file 12a at step S120, then sends only the most recent status information .O slashed.1 at time of transmitting the status mail .O slashed.2 to the console unit 20 via the mail server 19 at step S110. Therefore, even if the status code in the status information .O slashed.1 becomes temporarily the status code indicating WARNING or INFORMATION before the status mail .O slashed.2 is transmitted, the status code is not sent to the console unit 20 if the status is canceled when the status mail .O slashed.2 is transmitted. Then, the operator of the console unit 20 (agency) is relieved of the inconvenience of a temporary error.

Detailed Description Text (154):
If such a fatal error occurs, the agent unit 10 continues to monitor only the network printer P where the fatal error occurs in a time period (one minute) shorter than the normal monitor period (first time period T1) at steps S105 and S107, whereby the agent unit 10 can keep track of the status information .O slashed.1 more accurate than that in the normal state. If the fatal error is recovered from before the elapsed time since the fatal error occurrence exceeds one hour, immediately the agent unit 10 transmits status mail indicating the fact (fatal error recovery mail) to the console unit 20 via the mail server 19 at step S130. Therefore, the operator of the console unit 20 (agency) can cancel the emergency system adopted in response to the fatal error occurrence. In contrast, if the elapsed time since the fatal error occurrence exceeds one hour, immediately the agent unit 10 transmits status mail making a request for dispatching maintenance personnel (service call error mail) to the console unit 20 via the mail server 19 at steps S113 and S115. Therefore, the operator of the console unit 20 (agency) can dispatch maintenance personnel.

Current US Original Classification (1):
714/47

Previous Doc Next Doc Go to Doc#

US006430711B1

(12) **United States Patent**
Sekizawa

(10) **Patent No.:** **US 6,430,711 B1**
(45) **Date of Patent:** **Aug. 6, 2002**

(54) **SYSTEM AND METHOD FOR MONITORING THE STATE OF A PLURALITY OF MACHINES CONNECTED VIA A COMPUTER NETWORK**

(75) Inventor: **Hiroaki Sekizawa**, Suwa (JP)

(73) Assignee: **Seiko Epson Corporation**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/226,332**

(22) Filed: **Jan. 6, 1999**

(30) **Foreign Application Priority Data**

Jan. 6, 1998	(JP)	10-000694
Mar. 27, 1998	(JP)	10-081169
Mar. 27, 1998	(JP)	10-081170
Apr. 6, 1998	(JP)	10-093737
Apr. 6, 1998	(JP)	10-093738
Dec. 7, 1998	(JP)	10-347359

(51) **Int. Cl.**[7] **G06F 11/32**; G06K 15/00
(52) **U.S. Cl.** **714/47**; 358/1.14; 358/1.15
(58) **Field of Search** 714/47, 39; 709/217, 709/224, 223, 249, 238; 710/1, 105, 15, 62; 340/825.06, 286.02; 399/18; 700/169, 175, 108, 110; 370/908; 347/17, 101; 358/1.14, 1.15

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,251,858 A	*	2/1981	Cambigue et al.
5,077,582 A		12/1991	Kravette et al.
5,084,875 A		1/1992	Weinberger et al.
5,214,772 A		5/1993	Weinberger et al.
5,220,674 A	*	6/1993	Morgan et al.
5,305,199 A		4/1994	LoBiondo et al.
5,333,286 A		7/1994	Weinberger et al.
5,580,177 A	*	12/1996	Gase et al.
5,604,578 A		2/1997	Shibuya et al.
5,651,006 A		7/1997	Fujino et al.
5,727,135 A	*	3/1998	Webb et al.
5,859,778 A		1/1999	Kuroda et al.
5,982,994 A	*	11/1999	Mori et al.
6,088,816 A	*	7/2000	Nouri et al.

FOREIGN PATENT DOCUMENTS

JP	03-161765	7/1991
JP	04-256971	9/1992
JP	5-191405	7/1993
JP	05-236555	9/1993
JP	06-284150	10/1994
JP	06-348632	12/1994
JP	07-044630	2/1995
JP	07-288871	10/1995
JP	08-115125	5/1996
JP	08-241019	9/1996
JP	08-286854	11/1996
JP	09-134297	5/1997
JP	09-152815	6/1997
JP	9-188042	7/1997
JP	09-251356	9/1997

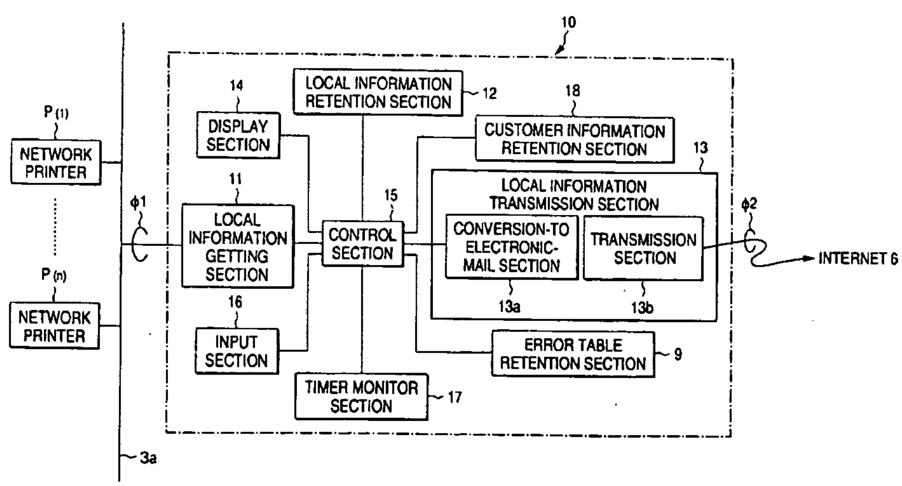
* cited by examiner

Primary Examiner—Gopal C. Ray
(74) *Attorney, Agent, or Firm*—Stroock & Stroock & Lavan LLP

(57) **ABSTRACT**

Each agent unit gets status information indicating the state of each of network printers connected by a LAN from the network printers every first time period. Whenever each agent unit gets the status information from the network printer, it overwrites a status log data file with the gotten status information. Each agent unit converts all status information stored in the status log data file into status mail of electronic mail and transmits the status mail to a mail server every second time period longer than the first time period. On the other hand, a console unit accesses the mail server and reads the status mail in a proper time period to the console unit.

69 Claims, 42 Drawing Sheets



Previous Doc Next Doc Go to Doc#
First Hit Fwd Refs

Generate Collection

L10: Entry 11 of 50 File: USPT Jul 23, 2002

DOCUMENT-IDENTIFIER: US 6425001 B1
TITLE: Network image scanning system which transmits image information from a scanner over a network to a client computer

Detailed Description Text (26):
A flags field 188 is an eight bit field in which individual bits identify different protocol states. Bit 0 is used to indicate an error in successfully transmitting a packet from the client computer to the scanner server. During file transfer from the scanner server to the client computer during the scan-to-application process, bit 1 is used to indicate that the information accompanying the packet header is the end of the file and bit 2 is used to indicate the end of a page of image information. Bit 3 is used to indicate that a sequence error has occurred and is used to request the transmitting entity to retransmit the packet which was not properly received. Each of the protocol commands uses the bit 0 and bit 3 flags and in FIGS. 7A-7L and 13A-13F, when the flags field indicates none, there are no special flags for this particular command, but the bit 0 and bit 3 flags are used.

Detailed Description Text (51):
Depending on the type of computer network 120 which is utilized by the present invention, different types of procedures can be performed to determine whether there is an available workgroup scanner on the network 120. When the network 120 is implemented using Novell NetWare, two methods of determining whether a scanner server exists on the network can be performed. A first method which can be used with the SPX/IPX protocol of Novell Netware has the client computer monitor Service Advertisement Protocol (SAP) packets which are transmitted by the various servers available on the network including the scanner server 130. These SAP packets are transmitted by each server approximately every 60 seconds in order to advertise the availability of the network servers. If this procedure is utilized by the client, it will be necessary for the client computer to monitor the existence of SAP packets from the scanner server 130. The SAP protocol also allows an inquiry request relating to available network services to be transmitted by a client which is responded to by a server. This inquiry mechanism is how client computers of the preferred embodiment of the invention determine the availability of network scanner servers.

Current US Original Classification (1):
709/217

Previous Doc Next Doc Go to Doc#

US006425001B2

(12) United States Patent
Lo et al.

(10) **Patent No.:** **US 6,425,001 B2**

(45) **Date of Patent:** **Jul. 23, 2002**

(54) **NETWORK IMAGE SCANNING SYSTEM WHICH TRANSMITS IMAGE INFORMATION FROM A SCANNER OVER A NETWORK TO A CLIENT COMPUTER**

(75) Inventors: **Robin Lo**, Saratoga; **Kanghoon Lee**, Fremont; **Lawrence Tremmel**, Riverbank; **David Stewart**, San Carlos; **Iwao Max Anzai**, Mountain View, all of CA (US)

(73) Assignees: **Ricoh Company, Ltd.**, Tokyo (JP); **Ricoh Corporation**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/825,971**

(22) Filed: **Apr. 5, 2001**

Related U.S. Application Data

(62) Division of application No. 09/222,314, filed on Dec. 29, 1998, now Pat. No. 6,256,662, which is a continuation of application No. 08/818,685, filed on Apr. 14, 1997, now Pat. No. 5,911,044.

(60) Provisional application No. 60/030,069, filed on Nov. 8, 1996.

(51) **Int. Cl.**^{7} **G06F 13/00**

(52) **U.S. Cl.** **709/217**; 709/329; 707/10; 707/104

(58) **Field of Search** 709/204, 207, 709/213, 216, 217, 230, 232, 236, 250, 313, 321, 329; 707/10, 100, 102, 104

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,257,369 A	*	10/1993	Skeen et al.	709/300
5,864,680 A	*	1/1999	Edblad et al.	709/238
5,911,044 A		6/1999	Lo et al.	709/203
5,933,598 A	*	8/1999	Scales et al.	709/216
6,218,718 B1	*	4/2001	Gregg et al.	257/421

* cited by examiner

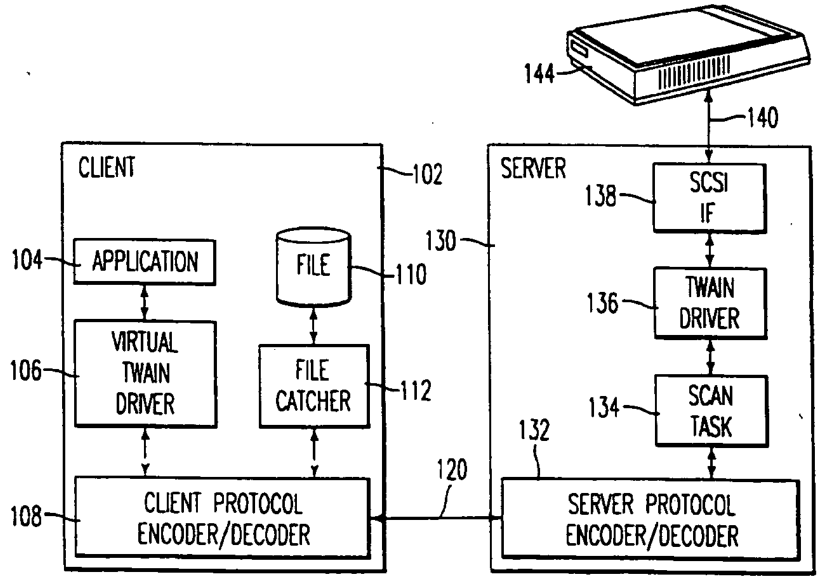
Primary Examiner—Viet D. Vu

(74) *Attorney, Agent, or Firm*—Oblon, Spivak, McClelland, Maier & Neustadt, P.C.

(57) **ABSTRACT**

A system and method for performing scanning operations using a scanner connected to a server computer and transmitting acquired images from the scanner server to a client computer. A scan-to-application process is utilized which allows control of the scanner or other image acquiring device which is connected to a scanner server using a virtual TWAIN driver which interfaces to an application program running in the client computer. Image files are also transmitted to a local file storage device of the client computer using a scan-to-file operation. A network protocol is used to implement both the scan-to-application and scan-to-file operation. Computer memories are utilized to store data structures or tables containing various information utilized during the file transfer procedures. Computer memories are also used to buffer and store the protocol packet headers and transmitted information.

23 Claims, 22 Drawing Sheets



L10: Entry 15 of 50 File: USPT Jul 10, 2001

DOCUMENT-IDENTIFIER: US 6259706 B1
TITLE: Communication controlling apparatus and recording medium for recording communication controlling programs

Brief Summary Text (5):
In a data transmission system, data is exchanged among a plurality of communication apparatuses such as SDH (Synchronous Digital Hierarchy) apparatuses through a plurality of communication lines. Normally, an SDH apparatus is provided with a monitoring processing unit for monitoring hardware failures of a communication line interface unit performing the role of an interface between a terminal and a communication line and failures occurring in a received signal. In the event of a failure, alarm information is transmitted to an external monitoring apparatus in accordance with a predetermined communication protocol. Receiving the alarm information, the external monitoring apparatus notifies a person in charge of maintenance of the existence of the failure by outputting the alarm information to a display unit. The person in charge of maintenance then issues a variety of control commands to the communication apparatus through a control processing unit employed in the communication apparatus in order to enhance communication reliability.

Detailed Description Text (25):
The clock processing unit 22 receives a clock signal supplied by an external clock generating circuit not shown in the figure and distributes the clock signal to the communication line interface unit 24, the monitoring processing unit 26, the control processing unit 28 and the external interface processing unit 30. The communication line interface unit 24 comprises a plurality of packages provided for interfaces such as a high speed communication line interface and a low speed communication line interface. Functions of the communication line interface unit 24 include relaying or multiplexing of principal signals to be transmitted as well as recognition of an operating state of a package employed therein as to which package is operating and detection of a principal signal failure and a hardware failure at a request made by the monitoring processing unit 26 besides notifying the monitoring processing unit 26 of alarming information on the failures. In addition, the communication line interface unit 24 carries out control processing for a package employed thereby in accordance with an instruction given by the control processing unit 28 and informs the control processing unit 28 of a result of the control processing.

Detailed Description Text (26):
The monitoring processing apparatus 26 monitors alarming states of the communication line interface 24 all the time and notifies an external monitoring apparatus 32 of the alarming states through the external interface processing unit 30 in accordance with a predetermined communication protocol. The control processing unit 28 carries out general control processing in the communication apparatus 20 in accordance with a control command received from the external monitoring apparatus 32 by way of the external interface processing unit 30 and transmits a result of the control processing to the external monitoring apparatus 32 through the external interface processing unit 30. The external interface processing unit 30 identifies a communication protocol adopted by the external

monitoring unit 32 and, if the communication protocol adopted by the external monitoring unit 32 is found different from the communication protocol adopted by the communication apparatus 20 and a control signal generated by a dip switch or the like as will be described later indicates that communication protocol conversion is to be implemented, the external interface processing unit 30 converts monitoring information coming from the monitoring processing unit 26 or a result of control processing coming from the control processing unit 28 into data conforming to the communication protocol adopted by the external monitoring apparatus 32, and transmits the data resulting from the conversion to the external monitoring apparatus 32.

Detailed Description Text (27):
In addition, the external interface processing unit 30 receives a control command from the external monitoring apparatus 32 and, if necessary, converts the control command into a command conforming to the communication protocol adopted by the communication apparatus 20 before passing on the command to the control processing unit 28. It should be noted that a communication protocol adopted by the external monitoring unit 32 can be converted into a communication protocol adopted by the communication apparatus 20 by using the same technique as the conversion of the communication protocol adopted by the communication apparatus 20 into the communication protocol adopted by the external monitoring unit 32. It is assumed, however, that a control command is transmitted by the external monitoring apparatus 31 to the control processing unit 28 in accordance with the same communication protocol as that adopted by the communication apparatus 20 in the present embodiment. The monitoring processing unit 26 and the control processing unit 28 are each connected to the external interface processing unit 30 by an internal bus. On the other hand, the external interface processing unit 30 is connected to the external monitoring apparatus 32 by a predetermined physical interface through connectors. In addition, the external interface processing unit 30 can be connected to 2 external monitoring apparatuses 32, that is, the existing external monitoring apparatus 32 having a certain communication protocol and a new external monitoring apparatus 32 with a communication protocol different from the communication protocol of the existing external monitoring apparatus 32. The new external monitoring apparatus 32 is used for replacing the existing one after its new communication protocol has been identified by the external interface processing unit 30.

Detailed Description Text (32):
1 The external monitoring apparatus 32 is designed so that, when the external monitoring apparatus 32 receives a message from the external interface processing unit 30 normally, the external monitoring apparatus 32 transmits an acknowledge response (ACK) to the external interface processing unit 30 and, when the external monitoring apparatus 32 does not receive a message from the external interface processing unit 30 normally due to the fact that the message has been transmitted not in accordance with a communication protocol adopted by the external monitoring apparatus 32, on the other hand, the external monitoring apparatus 32 transmits a non-acknowledge response (NAK) to the external interface processing unit 30. With the external monitoring apparatus 32 designed into such a scheme, the external interface processing unit 30 transmits a communication protocol identifying signal of its own for identifying the communication protocol adopted by the external monitoring apparatus 32 to the external monitoring apparatus 32 on its own initiative in accordance with a communication protocol supposed to be adopted by the external monitoring apparatus 32 when the external monitoring apparatus 32 is started. If an ACK response is received from the external monitoring apparatus 32, the external interface processing unit 30 judges the communication protocol, according to which the communication protocol identifying signal was transmitted to the external monitoring apparatus 32, to be the communication protocol adopted by the external monitoring apparatus 32. If no ACK response is received from the external monitoring apparatus 32, on the other hand, the external interface processing unit 30 repeats an operation to transmit the communication protocol

identifying signal to the external monitoring apparatus 32 on its own initiative in accordance with another communication protocol supposed to be adopted by the external monitoring apparatus 32 till an ACK response to the communication protocol identifying signal is received from the external monitoring apparatus 32 in which case the external interface processing unit 30 judges the communication protocol, according to which the communication protocol identifying signal was transmitted to the external monitoring apparatus 32, to be the communication protocol adopted by the external monitoring apparatus 32.

Detailed Description Text (33):
2 The external monitoring apparatus 32 is designed so that, when the external monitoring apparatus 32 receives a message from the external interface processing unit 30 normally, the external monitoring apparatus 32 transmits an acknowledge response (ACK) to the external interface processing unit 30 and, when the external monitoring apparatus 32 does not receive a message from the external interface processing unit 30 normally due to the fact that the message has been transmitted not in accordance with a communication protocol adopted by the external monitoring apparatus 32, on the other hand, the external monitoring apparatus 32 transmits a non-acknowledge response (NAK) to the external interface processing unit 30. With the external monitoring apparatus 32 designed into such a scheme, the external interface processing unit 30 transmits a message such as monitoring information, an alarm notification and a result of processing to the external monitoring apparatus 32 in accordance with a communication protocol. If an ACK response is received from the external monitoring apparatus 32, the external interface processing unit 30 judges the communication protocol, according to which the message was transmitted to the external monitoring apparatus 32, to be the communication protocol adopted by the external monitoring apparatus 32. If no ACK response is received from the external monitoring apparatus 32, on the other hand, the external interface processing unit 30 repeats an operation to transmit the message to the external monitoring apparatus 32 in accordance with another communication protocol till an ACK response to the message is received from the external monitoring apparatus 32 in which case the external interface processing unit 30 judges the communication protocol, according to which the message was transmitted to the external monitoring apparatus 32, to be the communication protocol adopted by the external monitoring apparatus 32.

Detailed Description Text (34):
3 There is also provided a method for identifying the communication protocol adopted by the external monitoring apparatus 32 from a signal which is transmitted by the external monitoring apparatus 32 when the external monitoring apparatus 32 is started. In this method, it is assumed that the external monitoring apparatus 32 is designed so that, when the external monitoring apparatus 32 is started, the external monitoring apparatus 32 transmits a signal to the communication apparatus 20 in order to establish communication with the communication apparatus 20.

Detailed Description Text (36):
The dip switch can be set to generate a control signal indicating whether the communication protocol conversion is to be or not to be implemented for the following reason. When the communication protocol of the external monitoring apparatus 32 has not been identified yet, for example, when a new external monitoring apparatus 32 has just been installed, the dip switch is set to generate a control signal indicating that the communication protocol conversion is not to be implemented because the correct communication protocol adopted by the external monitoring apparatus 32 is not known yet any way. Once the communication protocol adopted by the external monitoring apparatus 32 has been identified, however, the dip switch is set to generate a control signal indicating that the communication protocol conversion is to be implemented because the correct communication protocol adopted by the external monitoring apparatus 32 is now known. In addition, the external interface processing unit 30 can be connected to 2 external monitoring apparatuses 32, that is, the existing external monitoring apparatus 32 having a

certain communication protocol and a new external monitoring apparatus 32 with a communication protocol different from the communication protocol adopted by the existing external monitoring apparatus 32 for replacing the existing one after its new communication protocol has been identified by the external interface processing unit 30 as described earlier. With this scheme, the already known communication protocol is used for transmitting data to the existing external monitoring apparatus 32 till the new communication protocol is identified. After the new communication protocol has been identified, however, data can be transmitted to the newly installed external monitoring apparatus 32 in accordance with the identified communication protocol. As a result, the external monitoring apparatus 32 can be replaced with a new one without the need to temporarily halt the external monitoring apparatus 32. As a result, reliability of the communication and the network operation can be sustained.

Detailed Description Text (41):
FIG. 4 shows a flowchart representing operations carried out by the communication protocol identifying module 54 employed in the external interface processing unit 30 shown in FIG. 3. As shown in FIG. 4, the flowchart begins with a step S2, at which a communication protocol identifying signal for identifying the communication protocol adopted by the external monitoring apparatus 32 is transmitted to the external monitoring apparatus 32. The communication protocol identifying signal is a signal which only the external monitoring apparatus 32 adopting the protocol can receive normally. Examples of the communication protocol identifying signal is an alarm notification and a result of processing described earlier. In addition, an alarm notification or a result of processing used as a communication protocol identifying signal includes information indicating that the alarm notification or the result of processing is used specially as a communication protocol identifying signal and not an ordinary alarm notification or an ordinary result of processing. Receiving the communication protocol identifying signal, the external monitoring apparatus 32 checks the signal and transmits an ACK response to the communication protocol identifying signal to the external interface processing unit 30 if the signal is found received normally in accordance with its own communication protocol. If the communication protocol identifying signal is not received normally in accordance with its own communication protocol, on the other hand, the external monitoring apparatus 32 transmits a NAK response to the communication protocol identifying signal to the external interface processing unit 30.

Detailed Description Text (42):
The flow of the program 54 then goes on to a step S4 to form a judgment as to whether an ACK or NAK response is received from the external monitoring apparatus 32. If an ACK response is received from the external monitoring apparatus 32, the flow of the program 54 proceeds to a step S9. If a NAK response is received from the external monitoring apparatus 32, on the other hand, the flow of the program 54 proceeds to a step S6. At the step S6, the communication protocol identifying signal is retransmitted to the external monitoring apparatus 32 in accordance with another communication protocol. The flow of the program 54 then continues to a step S8 to form a judgment as to whether an ACK or NAK response is received from the external monitoring apparatus 32. If an ACK response is received from the external monitoring apparatus 32, the flow of the program 54 proceeds to the step S9. If a NAK response is received from the external monitoring apparatus 32, on the other hand, the flow of the program 54 returns to the step S6. At the step S9, the communication protocol used for transmitting the communication protocol identifying signal, for which an ACK response was received from the external monitoring apparatus 32, is judged to be the communication protocol adopted by the external monitoring apparatus 32. In this way, the communication protocol adopted by the external monitoring apparatus 32 can be identified.

Detailed Description Text (44):
A control signal generated by the dip switch not in the figure to indicate whether the communication protocol conversion is to be or not to be implemented as

described above is stored in a specific register or the like employed in the processor 40. Functions of the communication line interface unit 24 include relaying or multiplexing of principal signals to be transmitted as well as recognition of an operating state of a package employed therein as to which package is operating and detection of a principal signal failure and a hardware failure at a request made by the monitoring processing unit 26 in addition to notifying the monitoring processing unit 26 of alarming information on the failures. The monitoring processing apparatus 26 monitors alarming states of the communication line interface 24 all the time and notifies the external interface processing unit 30 of the alarming states.

Detailed Description Text (47):
At the step S16, the communication protocol converting module 60 is requested to convert the communication protocol adopted by the communication apparatus 20 into that adopted by the external monitoring apparatus 32. As will be described later, the communication protocol converting module 60 converts an alarm notification/monitoring information or a result of processing into data conforming to the communication protocol adopted by the external monitoring apparatus 32. At the step S18, the alarm notification/monitoring information or the result of processing received from the monitoring processing unit 26 or the control processing unit 28 respectively, or the data resulting from the communication protocol conversion carried out at the step S16 is transmitted to the external monitoring apparatus 32 by way of the upper level communication processing module 50 and the external monitoring apparatus communication processing sub-unit 46. The external monitoring apparatus 32 receives the alarm notification/monitoring information from the communication apparatus 20 monitored thereby and displays the alarm notification/monitoring information on an output unit such as a CRT to a person in charge of maintenance. On the other hand, the external monitoring apparatus 32 receives a control command from the maintenance person and passes on the control command to the communication apparatus 20. The external monitoring apparatus 32 then receives a result of processing transmitted by the communication apparatus 20 in response to the control command and displays the result of processing on the output unit such as the CRT. Since the alarm notification/monitoring information and the result of processing are transmitted in accordance with the communication protocol adopted by the external monitoring apparatus 32, they are received by the apparatus 32 normally.

Detailed Description Text (50):
FIG. 6 shows a flowchart representing operations carried out by a communication protocol converting module 60 employed in the external interface processing unit 30 shown in FIG. 3. As shown in FIG. 6, the flowchart begins with a step S20 at which the communication protocol of the external monitoring apparatus 32 identified by the communication protocol identifying module 54 shown in FIG. 4 is acquired from the communication protocol conversion controlling module 58. The flow of the program 60 then goes on to a step S22 at which communication protocol conversion data corresponding to the communication protocol acquired at the step S20 is read out from the communication protocol conversion data storing module 56. Then, the flow of the program 60 proceeds to a step S24 at which an alarm notification/monitoring information or a result of processing received from the monitoring processing unit 26 or the control processing unit 28 respectively is converted into data by using the protocol conversion data read out at the step S22. The control of execution is then returned to the calling protocol conversion controlling module 58 shown in FIG. 5. Assume that the communication apparatus 20 and the external monitoring apparatus 32 adopt communication protocols A and B respectively as shown in FIG. 7. In this case, the external interface processing unit 30 converts the communication protocol from communication protocol A into communication protocol B, allowing data conforming to communication protocol B transmitted by the communication apparatus 20 to be received normally by the external monitoring apparatus 32.

Detailed Description Text (61):
Much like the communication protocol conversion controlling module 58 shown in FIG. 3, the communication protocol conversion controlling module 102 controls communication protocol conversion, transmitting alarm notifications/monitoring information and results of processing to the external monitoring apparatus 84 by way of the upper level communication processing module 94 and the external monitoring apparatus communication processing sub-unit 90.

Detailed Description Text (63):
Much like the communication protocol converting module 60 of the first embodiment shown in FIG. 3, the communication protocol converting module 104 converts an alarm notification/monitoring information or a result of processing to be transmitted to the external monitoring apparatus 84 into data conforming to the communication protocol adopted by the external monitoring apparatus 84 in accordance with a command received from the communication protocol conversion controlling module 102. As a result, even in the case of a data transmission system wherein the communication apparatus 70 and the external monitoring apparatus 84 adopt communication protocols A and B respectively as shown in FIG. 10, the communication protocol converting unit 82 converts the communication protocol from communication protocol A into communication protocol B, allowing an alarm notification/monitoring information or a result of processing conforming to communication protocol B transmitted by the communication apparatus 70 to be received normally by the external monitoring apparatus 84.

Detailed Description Text (69):
The following is a description of the operation of the external interface processing unit 110 implemented by the third embodiment of the present invention with reference to FIG. 11. Basically, the operation of the external interface processing unit 110 is the same as the external interface processing unit 30 of the first embodiment shown in FIG. 3 except that there are differences in interface (between the processor 40 and the recording medium 112) between the former and the latter. When the recording medium 112 is inserted into the card interface unit or when the communication apparatus 20 shown in FIG. 2 is started, the processor 40 is started and the initialization processing module 52 is activated to carry out processing such as initialization of the memory space. Then, the communication protocol identifying module 54 is loaded by the initialization processing module 52 into the main memory for execution. The communication protocol identifying module 54, the communication protocol conversion controlling module 58 and the communication protocol converting module 60 operate in the same way as their counterparts employed in the external interface processing unit 30 of the first embodiment shown in FIG. 3 respectively, transmitting an alarm notification/monitoring information or a result of processing completing communication protocol conversion in accordance with a communication protocol adopted by the external monitoring apparatus 32 to the external monitoring apparatus 32. In addition, when a new communication protocol is introduced to the external monitoring apparatus 32, the external interface processing unit 110 allows the existing recording medium 112 to be taken out from the card interface unit to be replaced by a new recording medium 112 which keeps up with the new communication protocol.

Detailed Description Text (75):
The following is a description of the operation of the communication protocol converting apparatus 120, that is, the communication controlling apparatus implemented by the fourth embodiment of the present invention with reference to FIG. 12. Basically, the operation of the communication protocol converting apparatus 120 is the same as the communication protocol converting apparatus 82 of the second embodiment shown in FIG. 9 except that there are differences in interface (between the processor 86 and the recording medium) between the former and the latter. When the recording medium 122 is inserted into the card interface unit or when the communication apparatus 70 shown in FIG. 8 is started, the

processor 86 is started and the initialization processing module 96 is activated to carry out processing such as initialization of the memory space. Then, the communication protocol identifying module 98 is loaded by the initialization processing module 96 into the main memory for execution. The communication protocol identifying module 98, the communication protocol conversion controlling module 100 and the communication protocol converting module 102 operate in the same way as their counterparts employed in the communication protocol converting apparatus 82 of the second embodiment shown in FIG. 9 respectively, transmitting an alarm notification/monitoring information or a result of processing completing communication protocol conversion in accordance with a communication protocol adopted by the external monitoring apparatus 84 to the external monitoring apparatus 84.

Current US Cross Reference Classification (1):
709/228

Previous Doc Next Doc Go to Doc#

US006259706B1

(12) United States Patent
Shimada

(10) Patent No.: US 6,259,706 B1
(45) Date of Patent: Jul. 10, 2001

(54) COMMUNICATION CONTROLLING APPARATUS AND RECORDING MEDIUM FOR RECORDING COMMUNICATION CONTROLLING PROGRAMS

(75) Inventor: Junichi Shimada, Kawasaki (JP)

(73) Assignee: Fujitsu Limited, Kawasaki (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/054,104

(22) Filed: Apr. 2, 1998

(30) Foreign Application Priority Data

Oct. 23, 1997 (JP) 9-290617

(51) Int. Cl.[7] H04J 3/16; H04J 3/24; G06F 15/16

(52) U.S. Cl. 370/466; 709/228

(58) Field of Search 370/400, 401, 370/402, 464, 465, 466, 469; 710/11; 709/228

(56) References Cited

U.S. PATENT DOCUMENTS

5,500,860 *	3/1996	Perlman et al.	370/401
5,586,117 *	12/1996	Edem et al.	370/466
5,883,894 *	3/1999	Patel et al.	370/438

FOREIGN PATENT DOCUMENTS

6-2137945	6/1987	(JP) .
2198049	8/1990	(JP) .
4235439	8/1992	(JP) .
7245636	9/1995	(JP) .

* cited by examiner

Primary Examiner—Huy D. Vu
Assistant Examiner—Kevin C. Harper
(74) *Attorney, Agent, or Firm*—Helfgott & Karas, PC

(57) ABSTRACT

A communication controlling apparatus includes a receiving side communication protocol identifying means for determining a candidate communication protocol for a second apparatus. If an acknowledgment response is received from the second apparatus, a communication protocol is determined to be a candidate communication protocol for the second apparatus and, if no acknowledgment response is received, operations to convert a first signal into another signal conforming to another communication protocol supposed to be adopted by the second apparatus and to transmit the other signal to the second apparatus are repeated till an acknowledgment response to the other signal is received from the second apparatus. The apparatus also has a communication protocol converting means converting the first signal into another signal conforming to another communication protocol supposed to be adopted by the second apparatus, and a communication protocol conversion controlling means controlling the communication protocol converting means. If a first communication protocol is different from a protocol at the receiving side, a command is given to the communication protocol converting means to convert the first signal into another signal conforming to the communication protocol identified by the protocol identifying means at the receiving side.

14 Claims, 12 Drawing Sheets